Colegio de Administradores de Servicios de Salud

20 al 23 de junio de 2018

Integrando los Servicios de Salud
en Tiempos de Oportunidad

Business Continuity and Disaster Recovery

Pedro Cruz – Applications Sales Consultant

Rafael Vazquez – Applications Sales Executive

AT&T

Preparedness Planning for Your Business

Wiki Definition:

Disaster recovery (DR) and business continuity refers to an organization’s ability to recover from a disaster and/or unexpected event and resume operations. Organizations often have a plan in place (usually referred to as a "Disaster Recovery Plan" or "Business Continuity Plan") that outlines how a recovery will be accomplished.

Preparedness Planning for Your Business

Businesses and their staff face a variety of hazards:

- Natural hazards like floods, hurricanes, tornadoes, asteroids and earthquakes.
- Health hazards such as widespread and serious illnesses like the flu.
- Human-caused hazards including accidents, acts of violence, cybersecurity
- Technology-related hazards like power outages and equipment failure.

Submarine Fiber Landing Sites

- Data and voice connections to the world go through fiber landing sites in Miramar and Carolina.

XXIX CONVENCIÓN ANUAL CASS 2018

Aerial Fiber Delivers Most IP Services

- Susceptible to downed power poles and toppled trees

Utility Power Feeds Much Needed Energy

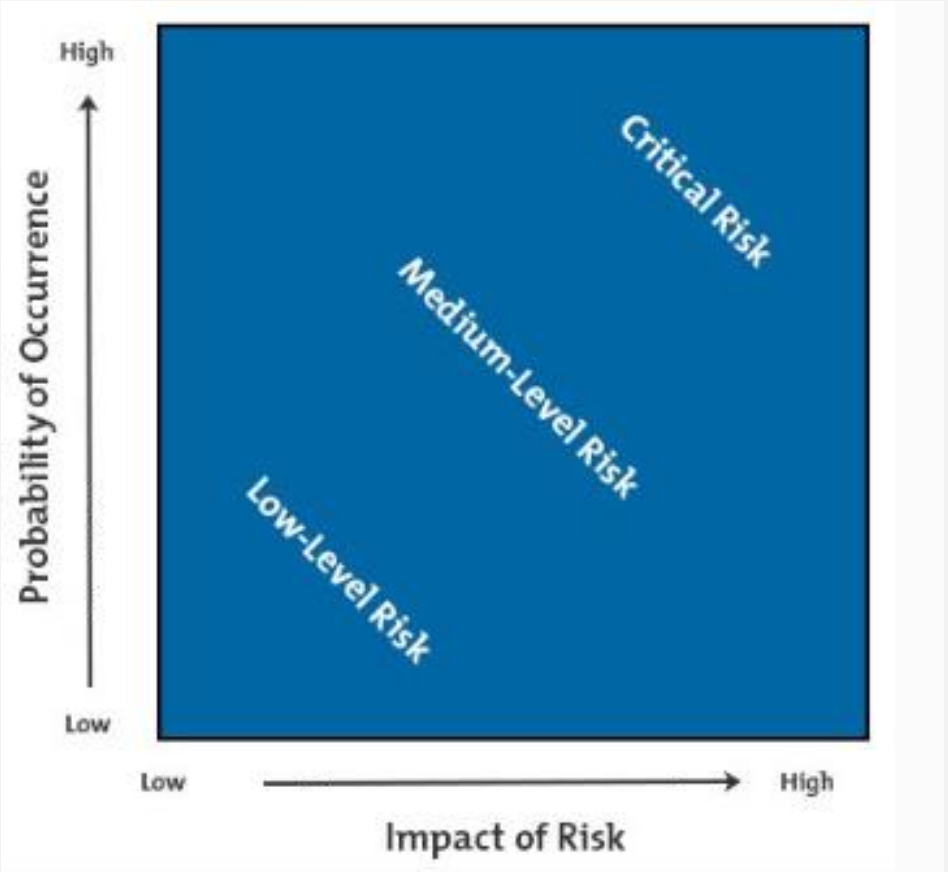
- With a weak and fragile utility power infrastructure it is very probable that power at base station sites will not be available or become unstable.

Inventory of Spare Equipment

- Correctly sized spare equipment inventory is difficult to determine

Be Ready!

- Identify Your Risks
- Develop A Plan
- Take Action



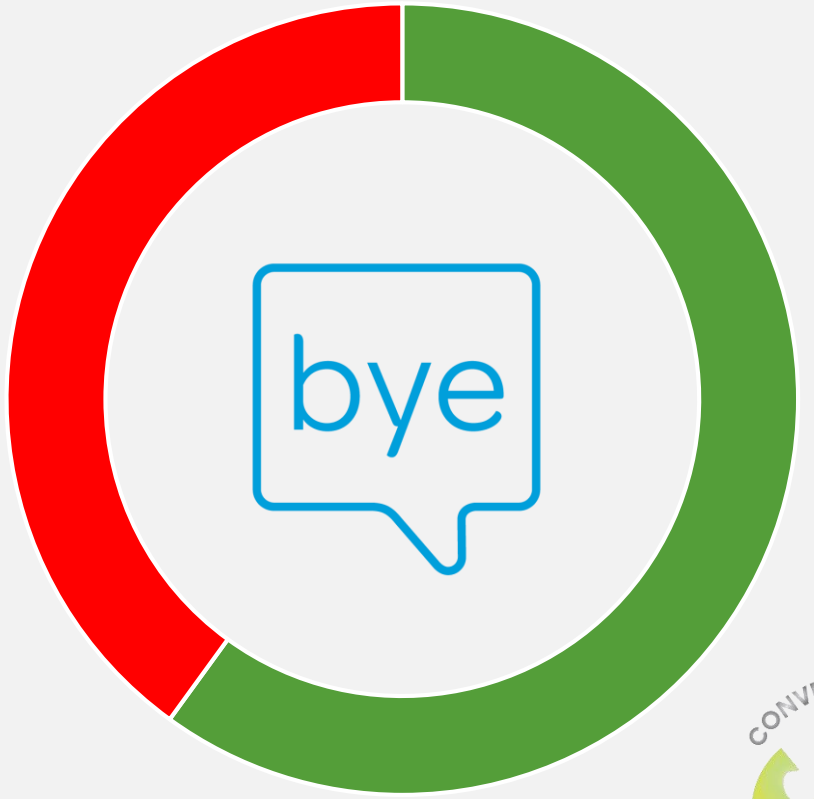
AT&T

XXIX CONVENCIÓN ANUAL CASS 2018

Small Businesses Are Prepared?

Nearly half of businesses must close during an unexpected event.

When an unexpected event occurs, **40% of small businesses aren't prepared and, as a result, must close their doors.**

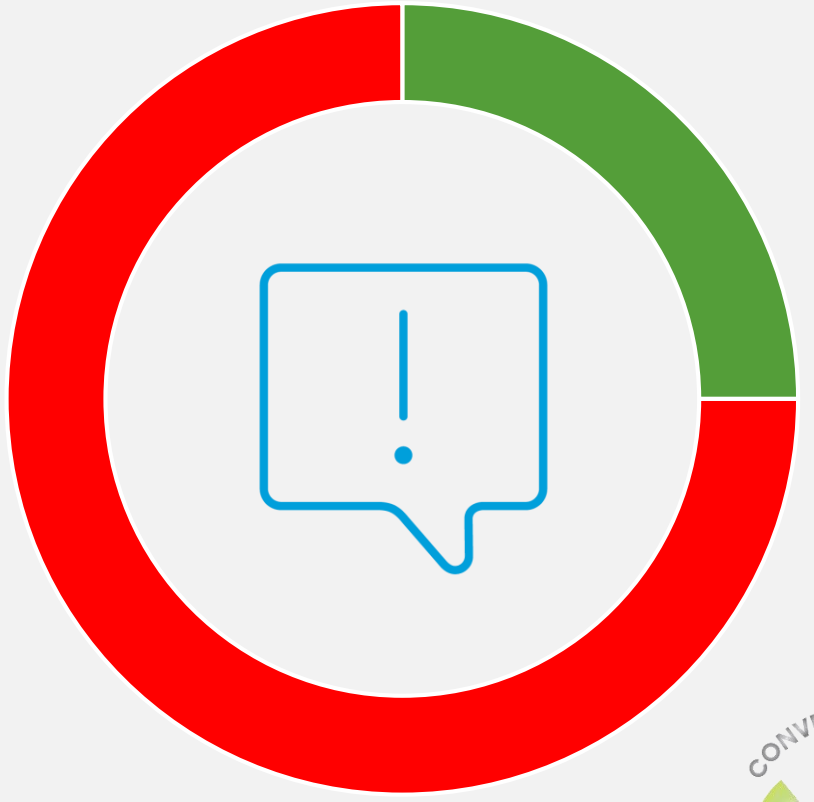


AT&T

XXIX CONVENCIÓN ANUAL CASS 2018

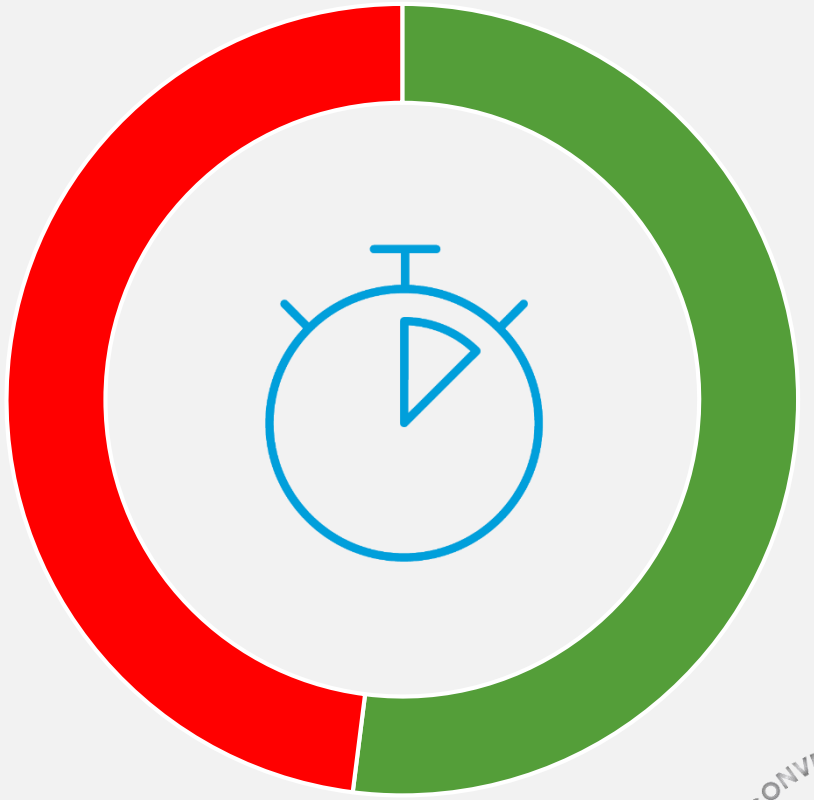
The majority of business don’t have a disaster recovery plan.

If you haven’t gotten around to creating a disaster recovery plan, you are not alone. **75% of small businesses are without a plan, according to a recent survey.** Creating a plan can minimize the impact during an unexpected event.



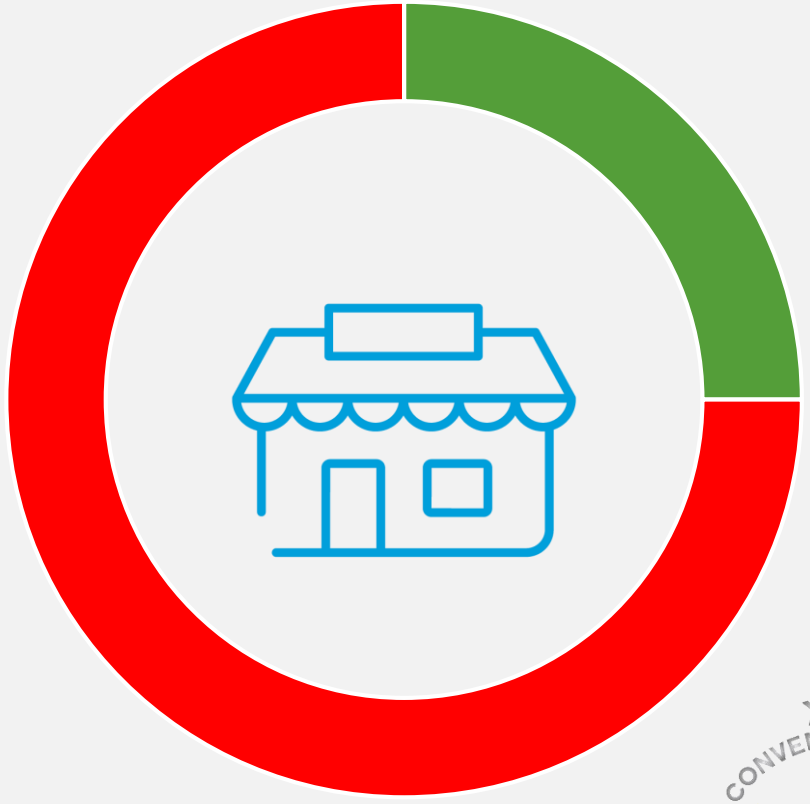
Recovery time is slow.

How long would it take to recover after an unexpected event? A week, a month or longer? **52% of SMBs report that it would take at least three months to recover from an unexpected disaster, which is enough time to cause a serious impact on business operations, revenue and growth.**



Closing the doors may be permanent.

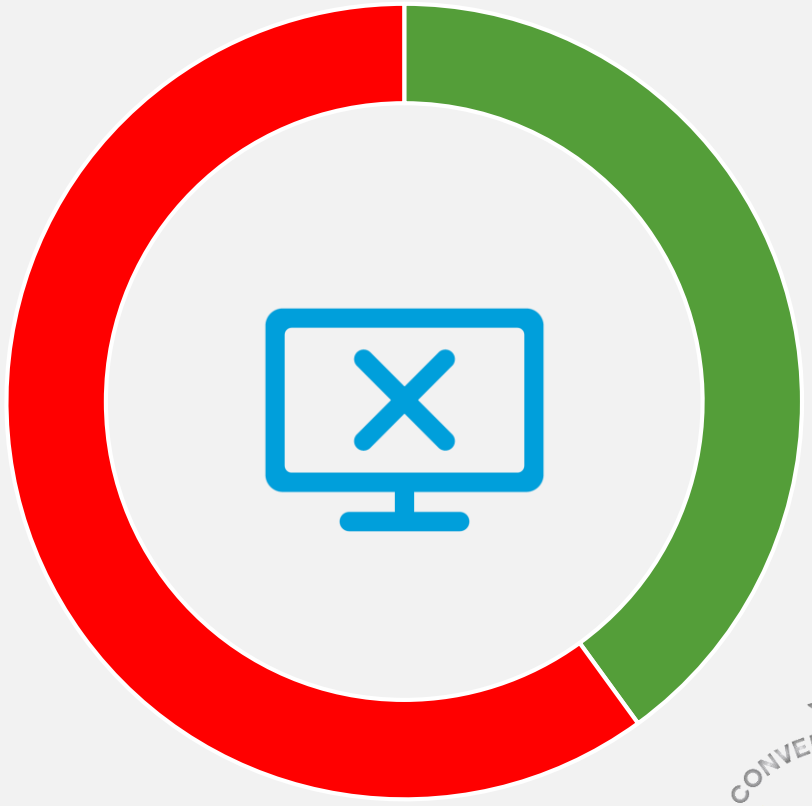
A large percentage of companies close during a disaster, but what's more, **only 25% of businesses that close reopen.** This highlights the importance of having a solid plan in place to minimize the risk of closing.



*DisasterSafety.org

Existing plans aren’t working.

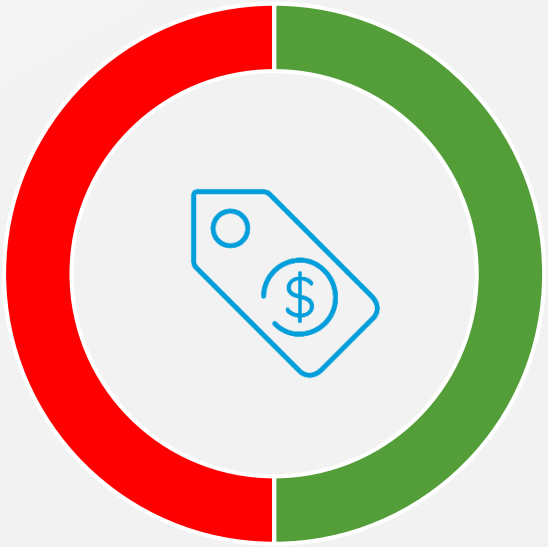
Even if you have a plan in place, updating that plan regularly is key to its success. **60% of respondents surveyed said that even though they prepared, their disaster recovery plans were not useful during the actual event.**



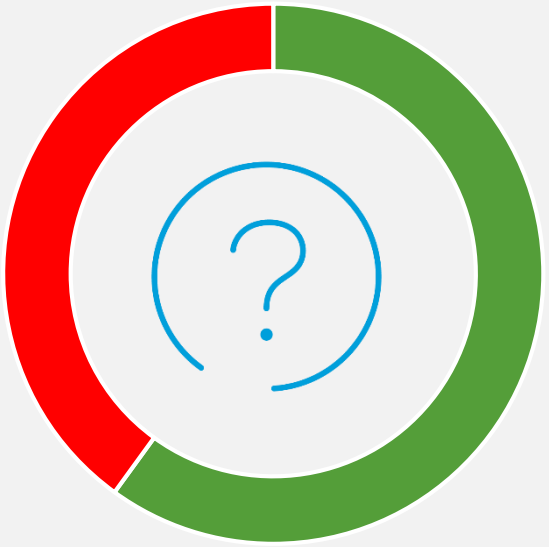
*drbenchmark.org

Sometimes the hardest part is getting started.

75% believe their plans are inadequate



50% believe solutions are too expensive



40% believe solutions are too complicated

Business Continuity Planning

When business is disrupted, it can cost money. Lost revenues plus extra expenses means reduced profits. Insurance does not cover all costs and cannot replace customers that defect to the competition. A business continuity plan to continue business is essential.

AT&T

XXIX CONVENCIÓN ANUAL CASS 2018

Development of a Business Continuity plan includes:

- Risk assessment
- Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement safeguards to recover critical business functions and processes.
- Organize a business continuity team and compile a business continuity plan to manage a business disruption.
- Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

Resource Required to Support Recovery Strategies

Recovery of a critical or time-sensitive process requires resources Resources can come from within the business or be provided by third parties. Resources include:

- Employees
- Office space, furniture and equipment
- Technology (computers, peripherals, communication equipment, software and data)
- Vital records (electronic and hard copy)
- Production facilities, machinery and equipment
- Inventory including raw materials, finished goods and goods in production.
- Utilities (power, natural gas, water, sewer, telephone, internet, wireless)
- Third party services
- Since all resources cannot be replaced immediately following a loss, managers should estimate the resources that will be needed in the hours, days and weeks following an incident.

What about IT?

Information technology (IT) includes many components such as networks, servers, desktop and laptop computers and wireless devices.

The ability to run both office productivity and enterprise software is critical.

Therefore, recovery strategies for information technology should be developed so technology can be **restored in time to meet the needs of the business**. Manual workarounds should be part of the IT plan so business can continue while computer systems are being restored.

IT Uses

Businesses use information technology to quickly and effectively process information.

Employees use:

- Email
- VoIP telephone systems
- Electronic data interchange transmit orders and payments
- Servers process information and store large amounts of data.
- Desktop PCs, laptops and wireless devices are used by employees to create, process, manage and communicate information.

IT Recovery Strategies

- Information technology systems **require hardware, software, data and connectivity.** Without one component of the "system," the system may not run. Therefore, **recovery strategies should be developed to anticipate the loss of one or more** of the following system components:
- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, routes, switches, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

What needs to be done?

- An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan.

  - **Priorities** and **recovery time objectives** for information technology should be developed during the business impact analysis.

  - Technology recovery strategies should be developed to **restore hardware, applications and data in time to meet the needs of the business recovery.**

Developing an IT Disaster Recovery Plan

- Businesses should develop an IT disaster recovery plan. **It begins by compiling an inventory of hardware (e.g. servers, desktops, laptops and wireless devices), software applications and data.** The plan should include a strategy to ensure that all critical information is backed up.
- Identify **critical software applications and data and the hardware required to run them**. Using standardized hardware will help to replicate and reimage new hardware. Ensure that copies of program software are available to enable re-installation on replacement equipment. **Prioritize hardware and software restoration**.
- Document the IT disaster recovery plan as part of the business continuity plan. **Test the plan periodically** to make sure that it works.

Business Continuity Impact Analysis

- Business continuity impact analysis identifies the effects resulting from disruption of business functions and processes

- Those functions or processes with the **highest potential operational and financial impacts** become priorities for restoration.

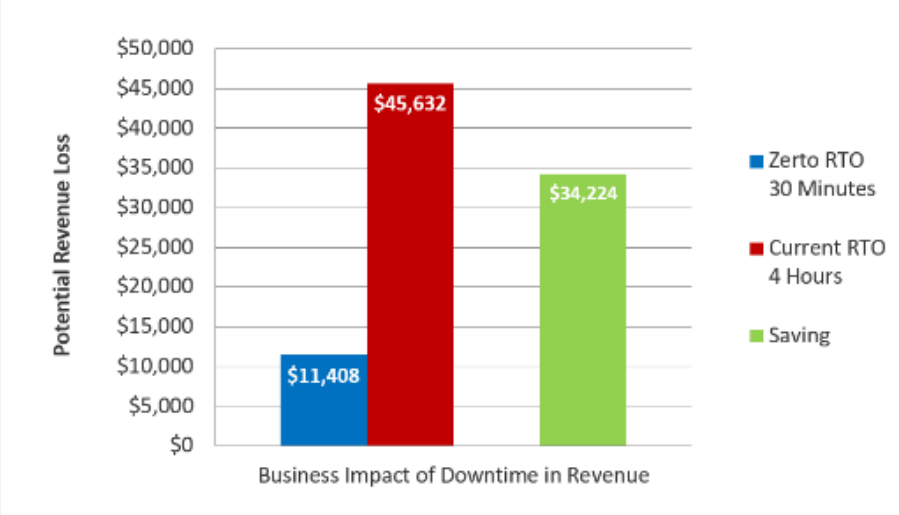
RTO Recovery Time Objectives “The time that it takes to recover data and applications”

- CRM System — 4 hour RTO
- Finance System — 4 hour RTO
- Email — 4 hour RTO
- File Servers — 4 hour RTO
- Directory Service — 2 hour RTO
- Print Servers — 24 hour RTO
- Dev Servers — 24 hour RTO

Recovery Strategies – Define Recovery Time Objectives

For example, if a facility is damaged, production machinery breaks down, a supplier fails to deliver or information technology is disrupted, business is impacted and the **financial losses** can begin to grow.

Recovery strategies are alternate means to **restore business operations to a minimum acceptable** level following a business disruption and are prioritized by the recovery time objectives (RTO) developed during the business impact analysis.



Internal Recovery Strategies

Many businesses have access to more than one facility. Hardware at an alternate facility can be **configured to run similar hardware and software applications** when needed.

Assuming data is backed up off-site or **data is mirrored** between the two sites, data can be restored at the alternate site and processing can continue.

Data Backup

- Businesses generate large amounts of data and data files are changing throughout the workday. **Data can be lost, corrupted, compromised or stolen through hardware failure, human error, hacking and malware.** Loss or corruption of data could result in significant business disruption.
- Data backup and recovery should be an integral part of the business continuity plan and information technology disaster recovery plan. Developing a data backup strategy begins with identifying **what data** to backup, selecting and implementing hardware and software backup procedures, **scheduling and conducting backups** and periodically validating that data has been accurately backed up.

Developing the Data Backup Plan

A) Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up

B) The plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server.

C) Data on the network server can then be backed up to cloud and/or redundant servers.

D) Backing up hard copy vital records can be accomplished by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

Options for Data Backup

- The frequency of backups, security of the backups and secure off-site storage should be addressed in the plan.
- Backups should be stored with the same level of security as the original data.
- Many vendors offer online data backup services including storage in the “cloud”.
- Data should be backed up as frequently as necessary to ensure that, if data is lost, it is not unacceptable to the business.
- The business impact analysis should evaluate the potential for lost data and define the “recovery point objective.”
- Data restoration times, or RTO, should be confirmed and compared with the IT and business function recovery time objectives.

Testing

Tests should be conducted to validate that business continuity recovery strategies will work. Tests should also be conducted to verify that systems and equipment perform as designed. Tests can take several forms, including the following:

- **Component -** Individual hardware or software components or groups of related components that are part of protective systems or critical to the operation of the organization are tested.
- **System -** A complete system test is conducted to evaluate the system's compliance with specified requirements. A system test should also include an examination of all processes or procedures related to the system being tested.
- **Comprehensive -** All systems and components that support the plan are tested. An example of a comprehensive test is confirming that IT operations can be restored at a backup site in the event of an extended power failure at the primary site.

Testing

- Tests of information technology systems and recovery strategies should be conducted in a manner **that resembles the everyday work environment**. If feasible, an actual test of the components or systems used should be employed. **Since tests can potentially be disruptive**, tests may be performed on systems that mimic the actual operational conditions.
- Inspection, testing and maintenance of building protection systems including fire detection, alarm, warning, communication, employee notification, emergency power supplies, life safety, fire suppression, pollution containment and others should be **conducted in accordance with manufacturers' instructions and regulatory requirements.** If a critical warning system or protection system fails, the consequences could be significant.

Testing Methods

- **Tabletop exercises:** are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios. The duration of a tabletop exercise depends on the audience, the topic being exercised and the exercise objectives. **Many tabletop exercises can be conducted in a few hours, so they are cost-effective tools to validate plans and capabilities.**
- **Functional exercises:** allow personnel to validate plans and readiness by performing their duties in a **simulated operational environment**. Activities for a functional exercise are scenario-driven, such as the failure of a critical business function or a specific hazard scenario. Functional exercises are **designed to exercise specific team members, procedures and resources** (e.g. communications, warning, notifications and equipment set-up).
- **A full-scale exercise:** is as close to the real thing as possible. It is a **lengthy exercise which takes place on location using, as much as possible**, the equipment and personnel that would be called upon in a real event. Full-scale exercises are conducted by public agencies. They often include participation from local businesses.

Exercises

Post-incident critiques often confirm that experience gained during exercises was the best way to **prepare teams to respond effectively** to an emergency.

Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident. **Exercises enhance knowledge of plans, allow members to improve their own performance and identify opportunities to improve capabilities to respond to real events.**

Exercises are a great method to:

- Evaluate the preparedness program
- Identify planning and procedural deficiencies
- Test or validate recently changed procedures or plans
- Clarify roles and responsibilities
- Obtain participant feedback and recommendations for program improvement
- Measure improvement compared to performance objectives
- Improve coordination between internal and external teams, organizations and entities
- Validate training and education
- Increase awareness and understanding of hazards and the potential impacts of hazards.
- Assess the capabilities of existing resources and identify needed resources

Crisis Communication Plan

- When an emergency occurs, the need to communicate is immediate. If **business operations are disrupted**, customers will want to know how they will be impacted.
- Regulators may need to be notified and local government officials will want to know what is going on in their community.
- **Employees and their families** will be concerned and want information. **Neighbors living near** the facility may need information—especially if they are threatened by the incident.
- All of these "audiences" will want information before the business has a chance to begin communicating.

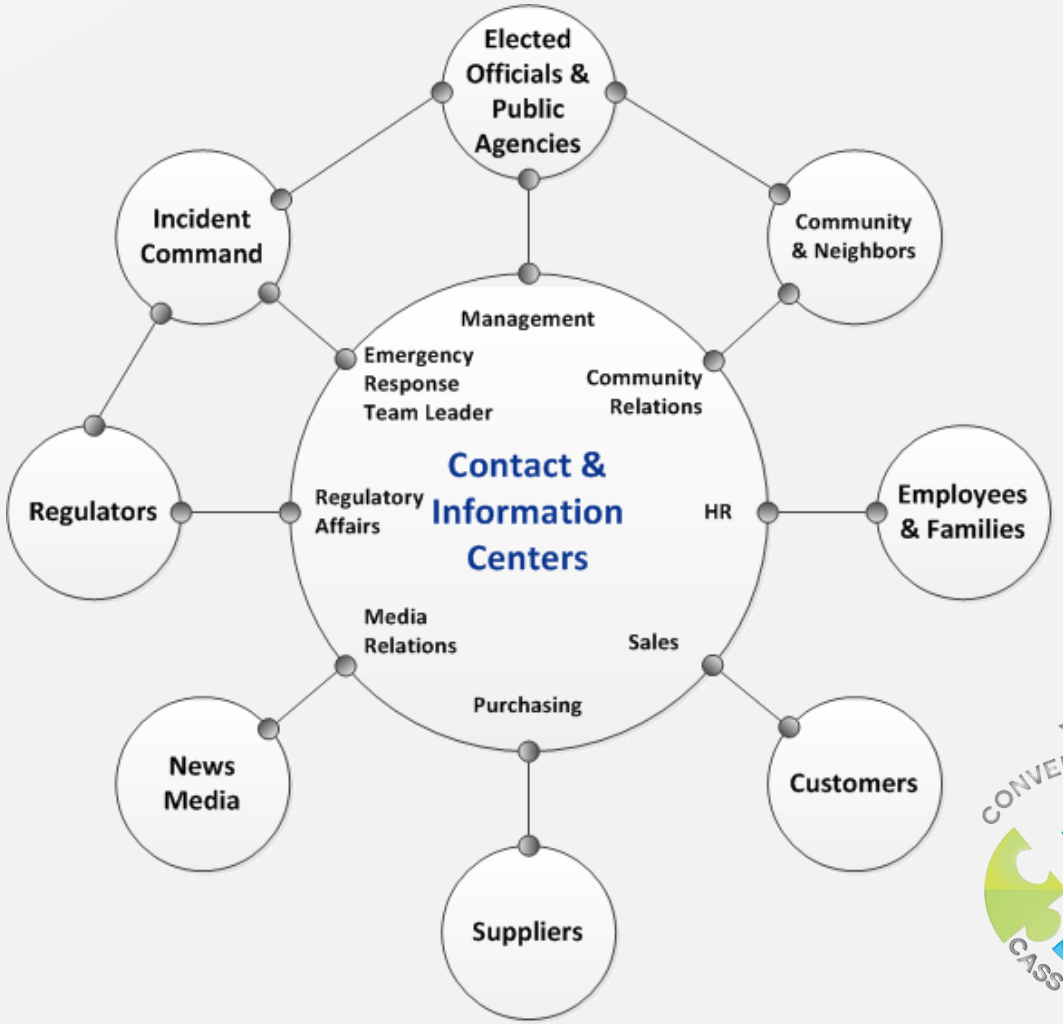
Audiences

- Understanding the audiences that a business needs to reach during an emergency is one of the first steps in the development of a crisis communications plan.
- The challenge is to identify potential audiences, **determine their need for information** and then identify **who within the business** is best able to communicate with that audience.
  - Customers
  - Survivors impacted by the incident and their families
  - Employees and their families
  - News media
  - Community—especially neighbors living near the facility
  - Company management, directors and investors
  - Government elected officials, regulators and other authorities
  - Suppliers

Crisis Communication Hub & Spoke

Communications before, during and following an emergency is bi-directional. Stakeholders or audiences will ask questions and request information.

The business will answer questions and provide information. This flow of information should be managed through a communications hub.



AT&T Business Continuity Survey

- Our business continuity study is based on a sample of 500 online surveys among Information Technology (IT) executives with primary responsibility for business continuity planning.
- The results show fears of potential security breaches and natural disasters, including extreme weather conditions

"We're seeing more and more major security events dramatically impact business operations across virtually every industry."

— Jason Porter, Vice President, Security Solutions, AT&T Business Solutions

AT&T

Key Findings From the Study:

Focus on Security

- Executives increasingly consider managing security requirements specific to mobile deployment (51%) and cloud (48%) as important business concerns.
- 54% of executives indicate that IT budgets have increased over the past two years, with “increasing data security” (31%) as one of the leading motivations for investing in new technologies.
- In order to respond to these growing concerns, businesses are investing in highly secure platforms across the entire IT landscape, with companies most frequently investing in cloud services (39%) and mobile applications (35%), followed closely by network security solutions (33%).

Aware of Current Event Types:

- 81% of companies indicate that their business continuity plan accommodates the possibility of a network security event, such as malware, phishing, bugs and malicious hackers.
- 63% of business leaders classify security breaches as their number one business concern in relation to overall security strategies.

Key Findings From the Study:

- (89%) indicate that they have a proactive approach to overall security
- (49%) claim they have a strong execution strategy in place
- (34%) have experienced a distributed denial-of-service (DDoS) attack in the past 24 months
- (50%) are currently taking proactive measures against protecting their company against DDoS attacks
- (26%) of companies have experienced an advanced persistent threat (APT) attack in the past 24 months
- 44% of respondents are taking a proactive approach to protecting their companies against advanced persistent threats.

AT&T

XXIX CONVENCIÓN ANUAL CASS 2018

Assess your own level of preparedness with the following questions

Assess Your Own Level of Preparedness

Mitigate risk, protect mission - critical resources

- Has the organization assessed the impact of a potential disruption?
- Has the organization analyzed which business processes, applications, facilities, suppliers, workgroups, or vital records are most critical?
- Has the organization created a strategy to recover from potential impacts?
- Are new scenarios, threats, and vulnerabilities addressed in our planning process?
- Has the organization developed and exercised a business continuity plan to mitigate business risk?

Assess Your Own Level of Preparedness

Mitigate risk, protect mission - critical resources

- Is this plan maintained and reviewed with the organization's response team on a regular basis?
- Is the plan approved by organization leadership?
- Are key locations hardened and facilities conditioned
- What physical and logical security measures are in place?
- Do the security measures in place also address potential exposure from cloud and mobile technology?

Assess Your Own Level of Preparedness

Meet regulatory requirements and customer service level agreements

- Does the organization or its business partners have regulatory mandated performance or availability service levels?
- Has the organization complied with all current or regulatory requirements or public policy mandates

Invest Wisely

- Has the organization quantified the potential costs of downtime or total business failure?
- Has the organization developed sound business cases to optimally invest in risk mitigation?

Disaster Recovery and Business Continuity Tools

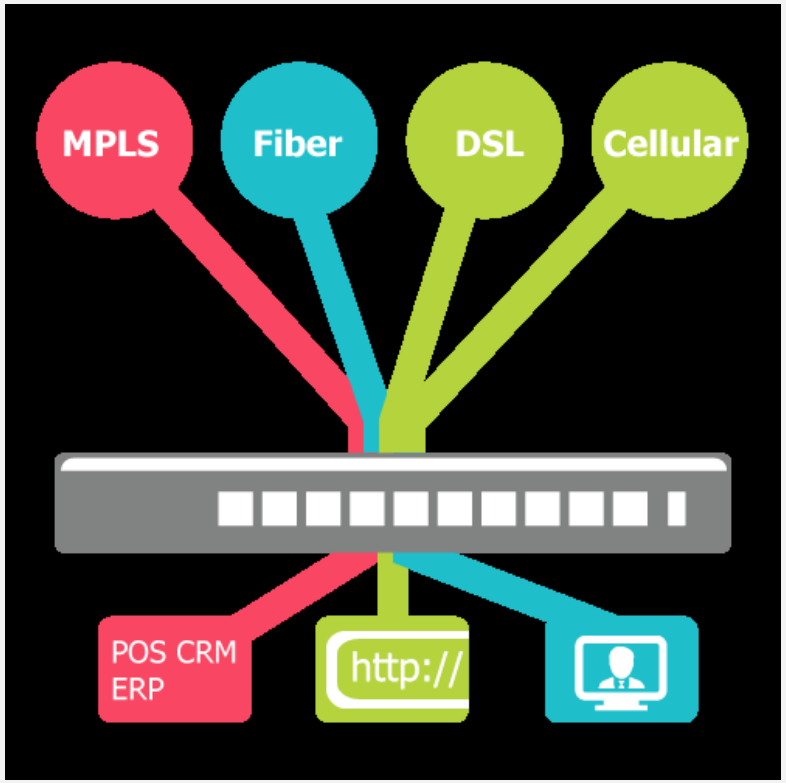
Is Everyone O.K.?

- Top priority is to account for every employee as quickly as possible
- Text “YESOK” and your Employee ID to 93765
- Company rep will travel to homes until everyone is accounted for

Multi Transport Solutions

- Fiber
- Copper
- Cellular
- Satellite
- “Flash drive”?

- MPLS vs SD-WAN



Data Center ‘Hardened’ IT Facilities

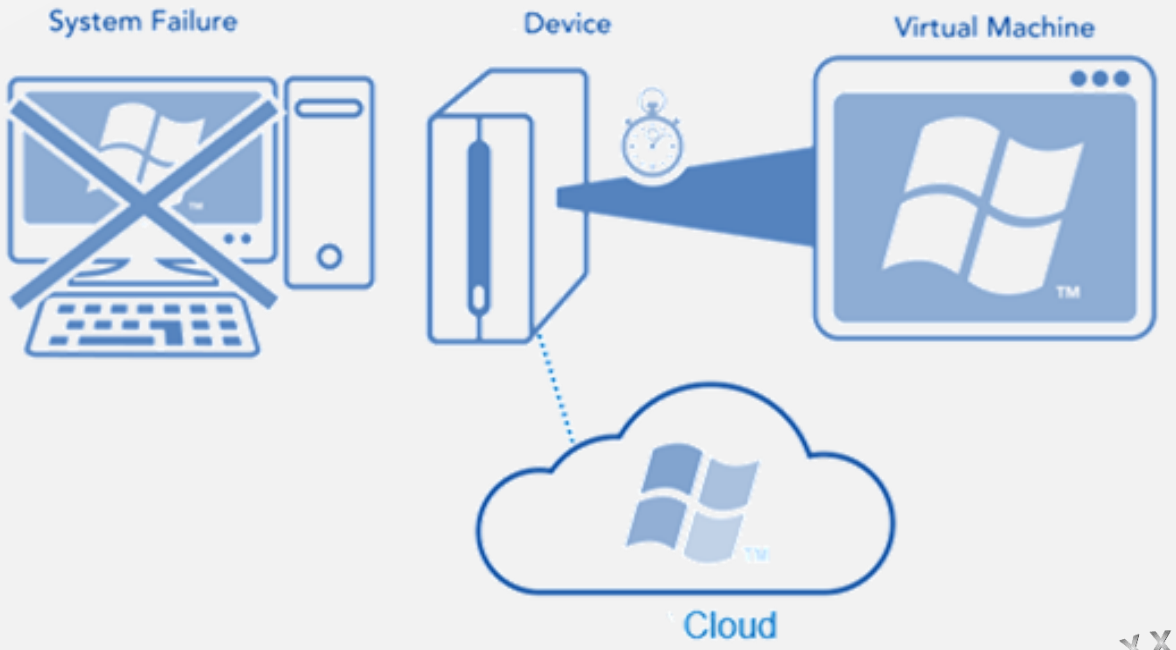
- Dual Power Generator + 1
- Dual UPS
- Dual HVAC
- FM-200 Extinguishing System
- Pipe Leak Detection
- VESDA System
- Secure and controlled environment

AT&T

XXIX CONVENCIÓN ANUAL CASS 2018

Hybrid Backup Solutions

- On Premise server and data backup
- Cloud backup
- Backup validation
- Ransomware detection
- Instant Virtualization from CPE & Cloud



Cloud Office Apps

- Work from anywhere and on any device
- Multi platform, iOS, Andorid, Mac Windows
- Redundant email servers in cloud
- Share documents through email and cloud
- Virtual conference rooms
- Add Secure email filters

Wireless Priority and Preemption

- FirstNet is a nationwide communications platform that provides a reliable, resilient, highly available wireless connection for emergency response.

- Priority and preemption capabilities are always on
- Reserved data and voice resources
- Mission critical applications
  - Incident Management
  - Geographic Information System (GIS)/mapping
  - Video streaming
  - Mission Critical Push-to-talk

Internet of Things – Remote Sensors

- Remote visibility of company assets
- IT Room – Temperature, water leak, voltage, unauthorized access
- Backup generator- temperature, hours of use, voltage, location

¡Gracias por su atención!